REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow. At the time of the outstanding Office Action, claims 1-14 were pending in the application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

Allowable Subject Matter:

Applicant thanks the Examiner for indicating that claims 3, 4, 6 and 7 contain allowable subject matter.

Prior Art Rejections:

Claims 1, 2, 5 and 13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,222,923 to Schwenk (hereinafter "Schwenk") in view of U.S. Patent 7,269,257 to Kitaya (hereinafter "Kitaya"). Claims 8 and 9 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk in view of Kitaya and further in view of U.S. Patent 7,155,611 to Wajs et al. (hereinafter "Wajs"). Claims 10, 11 and 14 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk in view of Wajs. These rejections are respectfully traversed for at least the following reasons.

Claims 1, 2, 5 and 13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk in view of Kitaya. Independent claim 1 recites a method of managing security keys that includes the step of "issuing keys to users from subtrees within the hierarchy upon the basis of their grouping." Independent claim 13 recites analogous features. Applicants respectfully submit that this feature is not taught by the cited prior art.

The Examiner relies on Schwenk to teach this feature of the invention as claimed. Schwenk is directed towards securing a system utilizing a key hierarchy. Specifically, Schwenk teaches issuing each individual customer a cryptographic key from a system operator or pay TV program provider (column 3, lines 25-27), and then generating group keys for each subset (column 3, lines 40-42) and transmitting the group keys with the help of the cryptographic keys. (column 3, lines 42-47). The group keys can be calculated by the user by

using their individual cryptographic keys (column 3, lines 48-51). There is no teaching or suggestion in Schwenk that a cryptographic key is issued from the subtree upon the basis of their grouping. Schwenk fails to explicitly teach or disclose that the group key is issued to the user from the subdomain or subset of the tree.

The Examiner cites the following passage of Schwenk to teach "issuing keys to users from subtrees within the hierarchy upon the basis of their grouping:"

> "In addition, a new common key SK' is also generated. The procedure for generating the group key and a common key has already been explained in detail previously. **The newly generated cryptographic keys are sent out to the individual customers again and stored at the central location.** The pirate, who is customer 4 in our case, is now forced to copy the new group key GK_2' and distribute it to third parties. As soon as the central location obtains the copied group key GK_2', it is stored again in the central storage device. Subsequently the intersection of the subset to which the cryptographic group key GK_2 is assigned and the subset to which the cryptographic group key GK_2' is assigned is determined. Since the subset formed at time 1 (see FIG. 1) contains customers 3 and 4, and the subset formed at time 2 (see FIG. 2) contains customers 2 and 4, the dishonest customer 4 results as the intersection. The central location now knows the identity of the dishonest customer and can bar him from using the system, for example, by blocking his individual cryptographic key PK_4. Although the key hierarchies illustrated in FIGS. 1 and 2 include only four customers, key hierarchies of any size can be used, in which case, of course, the cost of finding a dishonest customer also increases, since the number of groups is greater." (column 4, lines 17-38)

This passage teaches how Schwenk would be able to identify a pirate. However, there is no teaching or suggestion that the group key is issued from a subdomain of the tree. Thus, Applicants respectfully submit that Schwenk fails to teach or disclose a method of managing security keys that includes the step of "issuing keys to users from subtrees within the hierarchy upon the basis of their grouping."

Kitaya fails to make up for the deficiencies of Schwenk as detailed above. Kitaya is directed towards generating and distributing an enabling key block corresponding to data processing ability of a device and to manage devices by dividing a hierarchical key tree structure. (Abstract). There is no teaching or suggestion in Kitaya of a method of managing security keys that includes the step of "issuing keys to users from subtrees within the hierarchy upon the basis of their grouping."

Thus, if this rejection is maintained, the Examiner is respectfully requested to point out where this feature is found in either Schwenk or Kitaya.

The dependent claims that depend from the independent claims are also patentable for at least the same reasons as the independent claims on which they ultimately depend. In addition, they recite additional patentable features when considered as a whole.

Claims 10, 11 and 14 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk in view of Wajs. Independent claim 10 recites a method of managing security key distribution that includes the step of "defining levels of service provision" "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled" and "for at least one level of service provision, allocating dummy keys which do not provide security for the provision of the service."

The Examiner relies on Schwenk to teach "defining levels of service provision" and "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled." The following passage of Schwenk details the level of service provided to customer and the formation of subsets of customers:

> "For example, let us assume that only customers 1, 2, 3, and 4 are authorized to receive the TV program, but not customer 5. In order to achieve this distribution of authorizations, customers 1 through 4 are grouped in the next higher hierarchical level--i.e., the second level preferably to form two subsets with two customers each." (column 3, lines 34-40)

However, there is no teaching or suggestion in this passage that the subsets are indicative of a level of service provision. Rather, Schwenk teaches that the subsets are

merely defined by size. (column 3, lines 13-14). Further, the allocation of a group key to users in the subset is not indicative to a service provider of the level of service to which the user is entitled. Rather, as evidenced in the passage cited above with reference to levels of service provision, all customers in the subsets are authorized to receive the TV program. Further, Schwenk fails to teach or disclose further authorizations with regards to viewing capability or other features that would distinguish levels of service provision. Thus, Schwenk fails to teach or disclose a method of managing security key distribution that includes the step of "defining levels of service provision" "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled" and "for at least one level of service provision, allocating dummy keys which do not provide security for the provision of the service."

Wajs fails to make up for the deficiencies of Schwenk as detailed above. Wajs is directed towards a conditional access system for broadcast applications. (Abstract). Access is granted conditionally to subscribers with a conditional access module and a smart card. (column 3, lines 45-60). However, Wajs fails to teach or disclose defining levels of service provision for those broadcast applications. Access is either granted or denied, without any distinction as to different services provided to different subscribers. Thus, Wajs also fails to teach or disclose a method of managing security key distribution that includes the step of "defining levels of service provision" "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled" and "for at least one level of service provision, allocating dummy keys which do not provide security for the provision of the service."

Thus, if this rejection is maintained, the Examiner is respectfully requested to point out where this feature is found in either Schwenk or Wajs.

The dependent claims that depend from the independent claims are also patentable for at least the same reasons as the independent claims on which they ultimately depend. In addition, they recite additional patentable features when considered as a whole.

Conclusion:

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 C.F.R. § 1.25. Additionally, charge any fees to Deposit Account 08-2025 under 37 C.F.R. § 1.16 through § 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Date 6/30/06

By _____

FOLEY & LARDNER LLP
Customer Number: 22879
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

William T. Ellis
Attorney for Applicant
Registration No. 26,874

Ramya Ananthanarayanan
Agent for Applicant
Registration No. 59,597